UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,539	03/02/2000	Simon Robert Walmsley	AUTH01US	4602

7590 03/11/2005

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain, 2041
AUSTRALIA

EXAMINER	
NGUYEN, NGA B	

ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 03/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/517,539	WALMSLEY ET AL.	
	Examiner	Art Unit	
	Nga B. Nguyen	3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 August 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 4, 2004 has been entered.

2. Claims 1-12 are pending in this application.

Response to Arguments/Amendment

3. Applicant's arguments with respect to claims 1-12 have been fully considered but are moot in view of new grounds of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 2, 4, 6, 7, and 11 are rejected under 35 U.S.C. 102(e) as being anticipated by Lee, U.S. Patent No. 5,923,759.

Regarding to claim 1, Lee discloses a validation protocol for determining whether an untrusted authentication chip (column 4, lines 53-65, smart cards 142, 144, or 146 is equivalent to the untrusted authentication chip) is valid, or not, including the steps of:

generating a random number in a trusted authentication chip (column 6, lines 37-41, processor 122 generates a random number, processor 122 is equivalent to the rusted authentication chip);

applying, in the trusted authentication chip, a keyed one way function to the random number using a first key from the trusted authentication chip to produce a first encrypted outcome (column 6, lines 57-60, the processor 122 encrypts the random number based upon an algorithm and an identifying key stored in memory 126 and returns the encrypted random number to the card; column 7, lines 1-15, symmetrical algorithm is one way function);

applying, in the untrusted authentication chip, a keyed one way function to the random number using a second secret key from the untrusted authentication chip to produce a second encrypted outcome (column 6, lines 40-46, the card encrypts the random number based upon an algorithm and an "internal key" stored in the card and returns the encrypted random number to the processor 122);

comparing the first encrypted outcome and the second encrypted outcome, without knowledge of the first key or the second key, and in the event of a match considering the untrusted chip to be valid (column 6, lines 60-67, the card compares the original random number with the decrypted random number without the knowledge of the "internal key" stored in the card; column 6, lines 46-52; the processor 122 compares

the original random number and the decrypted random number without the knowledge of the identifying key stored in memory 126);

otherwise considering the untrusted chip to be invalid (column 6, lines 50-51, 65-67).

Regarding to claim 2, Lee discloses the first and second keys are kept secret (column 6, lines 40-46, the "internal key" stored in the card; column 6, lines 55-60, the identifying key stored in memory 126).

Regarding to claim 4, Lee discloses the keyed one-way function is a symmetric cryptograph, a random number sequence, or a message authentication code (column 7, lines 1-15).

Claims 6, 7, 11 have similar limitations found in claims 1, 2, 4 above, therefore, are rejected by the same rationale.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 3 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee, U.S. Patent No. 5,923,759, in view of Abraham et al (hereinafter Abraham), U.S. Patent No. 4,799,061.

Regarding to claims 3 and 10, Lee does not disclose the domain of the random numbers generated is non-deterministic. However, Abraham discloses the domain of the random numbers generated is non-deterministic (column 3, lines 9-13, the random numbers generated is non-deterministic because each challenge requires the use of a new random number). Therefore, it would have been obvious to modify Lee's to adopt the teaching of Abraham above for the purpose of providing high security level because each challenge requires a new random number, thus the unauthorized person cannot easily to predict the random number.

8. Claims 5, 8, 9, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee, U.S. Patent No. 5,923,759, in view of Thomlinson et al (herein after Thomlinson), U.S. Patent No. 5,778,069.

Regarding to claims 5 and 12, Lee discloses the one-way function is a symmetric cryptographic function (column 7, lines 1-15), but Lee does not disclose the key has a minimum size of 128 bits. However, Thomlinson discloses the key has a minimum size of 128 bits (column 5, lines 59-65). Therefore, it would have been obvious to modify Lee's to adopt the teaching of Thomlinson above for the security purpose because producing the encryption and decryption keys with larger bits makes the unauthorized person cannot easily to guess the keys.

Regarding to claims 8 and 9, Lee does not disclose the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed, and for a group of authentication chips, each

chip has a different initial seed, so that the first call to each chip requesting a random number will produce different results for each chip in the group. However, Thomlinson discloses the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed (column 6, lines 36-60). Moreover, it is well known to use a different initial seed for each chip in the group of chip. Therefore, it would have been obvious to modify Lee's to adopt the teaching of Thomlinson above for the purpose of providing high security level because each random number is generated from a new seed and each chip has a different initial seed, thus the unauthorized person cannot easily to predict the random number.

Conclusion

9. Claims 1-12 are rejected.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner Nga B. Nguyen whose telephone number is (703) 306-2901. The examiner can normally be reached on Monday-Thursday from 9:00AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung S. Sough can be reached on (703) 308-0505.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 306-1113.

11. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

C/o Technology Center 3600

Washington, DC 20231

Or faxed to:

(703) 872-9326 (for formal communication intended for entry),

or

(703) 308-3691 (for informal or draft communication, please label "PROPOSED" or "DRAFT").

Hand-delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, VA, Seventh Floor (Receptionist).

Nga B. Nguyen

Nga Nguyen

March 1, 2005